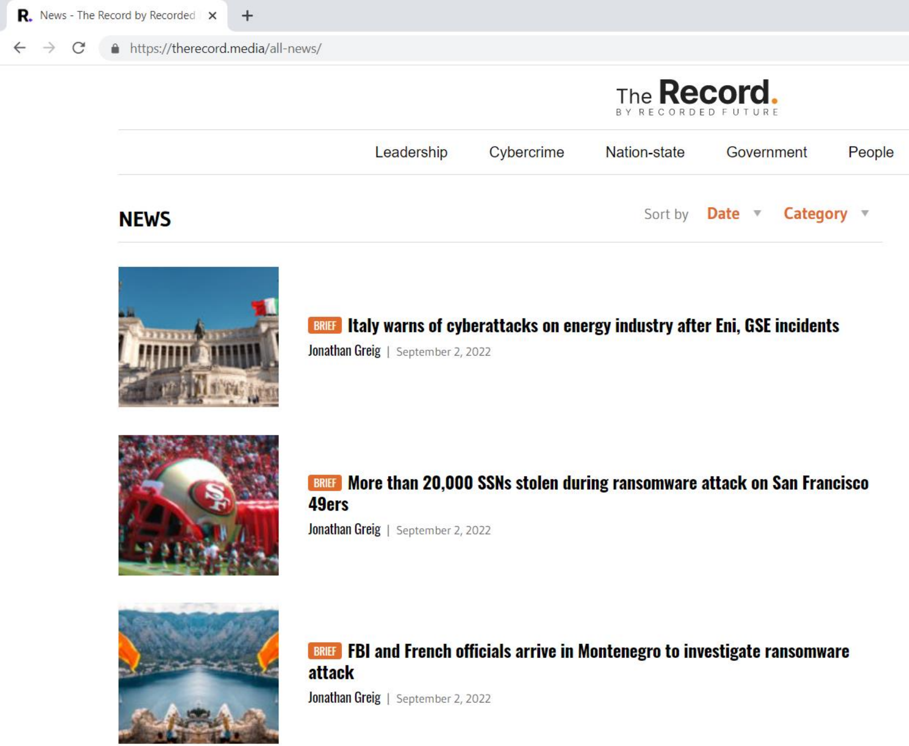
IT-Security (ITS) B1

DIKU, E2022

It’s all about:



News - The Record by Recorded

https://therecord.media/all-news/

The Record. BY RECORDED FUTURE

Leadership Cybercrime Nation-state Government People

NEWS

Sort by Date ▾ Category ▾

BRIEF **Italy warns of cyberattacks on energy industry after Eni, GSE incidents**
Jonathan Greig | September 2, 2022

BRIEF **More than 20,000 SSNs stolen during ransomware attack on San Francisco 49ers**
Jonathan Greig | September 2, 2022

BRIEF **FBI and French officials arrive in Montenegro to investigate ransomware attack**
Jonathan Greig | September 2, 2022

Today's agenda

Part 1.

Course overview

Security defined

Part 2.

Who hacks?

Lectures

Lectures

Mondays and Fridays, at 10-12, Lille UP1

Instructors

Martin Elsman (course organiser)
Troels Langkjær
Carsten Jørgensen

Lecture plan

Week	Date	Time	Instructor	Topic
36	05 Sep	10-12	TL	Security concepts and principles
	09 Sep	10-12	TL	Cryptographic building blocks
37	12 Sep	10-12	TL	Key establishment and certificate management
	16 Sep	10-12	CJ	User authentication, IAM
38	19 Sep	10-12	CJ	Operating systems security, web, browser and mail security
	23 Sep	10-12	CJ	IT security management and risk assessment
39	26 Sep	10-12	TL	Software security - exploits and privilege escalation
	30 Sep	10-12	TL	Malicious software
40	03 Oct	10-12	CJ	Firewalls and tunnels, security architecture
	07 Oct	10-12	CJ	Cloud and IoT security
41	10 Oct	10-12	TL	Intrusion detection and network attacks
	14 Oct	10-12	TL	Forensics
42				Fall Vacation - No lectures
43	24 Oct	10-12	CJ	Privacy and GDPR
	28 Oct	10-12	CJ	Privacy engineering
44	31 Oct	10-11	Guest	Special topic
		11-12	TL,CJ	Exam Q/A

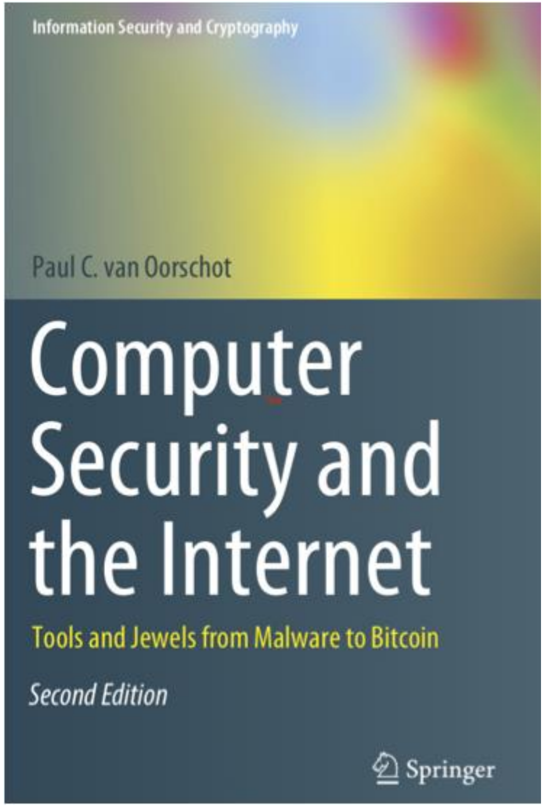
https://github.com/diku-its/its-e2022/blob/main/lectureplan2022.md

Course book

Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin, Second Edition by Paul C. van Oorschot. Springer, 2021

+ a few online resources

Note: Lectures focus on the big picture and are not 1:1 with the reading material



Information Security and Cryptography

Paul C. van Oorschot

Computer Security and the Internet

Tools and Jewels from Malware to Bitcoin

Second Edition

Springer

Assignments

There are 6 weekly assignments during the course.

Week	Due date	Assignment
36	None	Assignment 0
37	18 Sep	Assignment 1
38	25 Sep	Assignment 2
39	02 Oct	Assignment 3
40	09 Oct	Assignment 4
41	16 Oct	Assignment 5
42	23 Oct	Possible re-handin of one assignment (1-4)
43	30 Oct	Assignment 6

Note: pass/fail; groups of up to 3; expect at least 66 % of an assignment correct to pass; re-handin of only one.

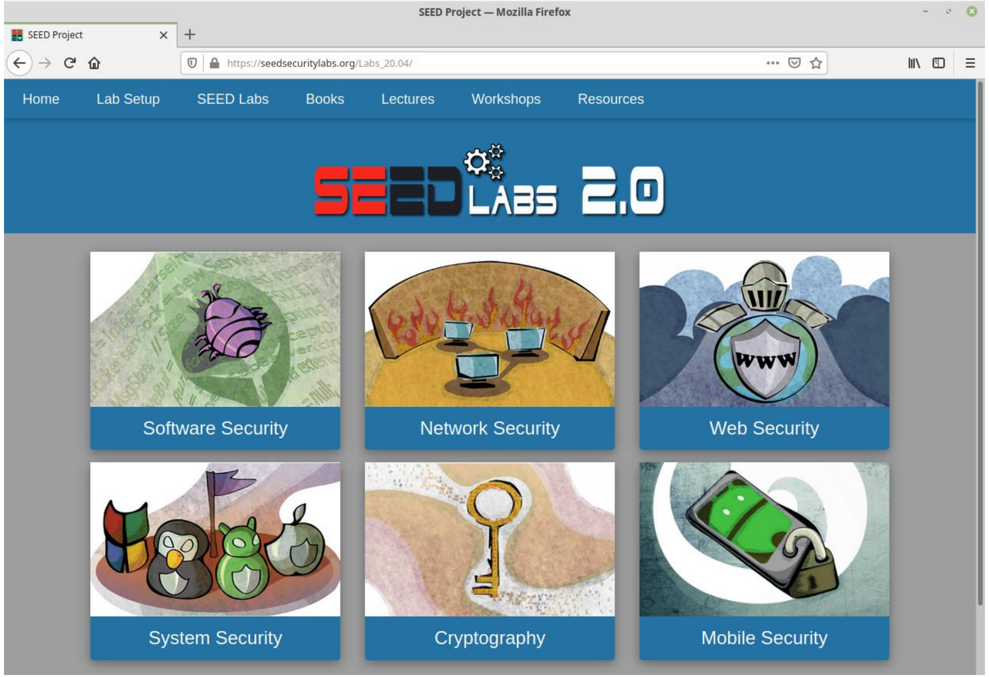
Assignments

There are 6 weekly assignments during the course.

Week	Due date	Assignment	Topic
36	None	Assignment 0	Getting ready
37	18 Sep	Assignment 1	Encryption
38	25 Sep	Assignment	Environment variables and more
39	02 Oct	Assignment 3	Web attacks
40	09 Oct	Assignment 4	Firewalls
41	16 Oct	Assignment 5	Network attacks
42	23 Oct	Possible re-handin of one assignment (1-4)	
43	30 Oct	Assignment 6	Forensics

Note: pass/fail; groups of up to 3; expect at least 66 % of an assignment correct to pass.

SEED Labs



SEED Project — Mozilla Firefox

Exercise classes

Exercise classes

Tuesdays, at 13-17, BIOcenter 2-0-17, 2-1-17, 2-2-17, and 4-0-10

TAs

- Morten Risum Pedersen
- Niels Gøttge Lerche Hansen
- Frederik Lunn Berthelsen
- Andreas Lajer Mikkelsen

Exam

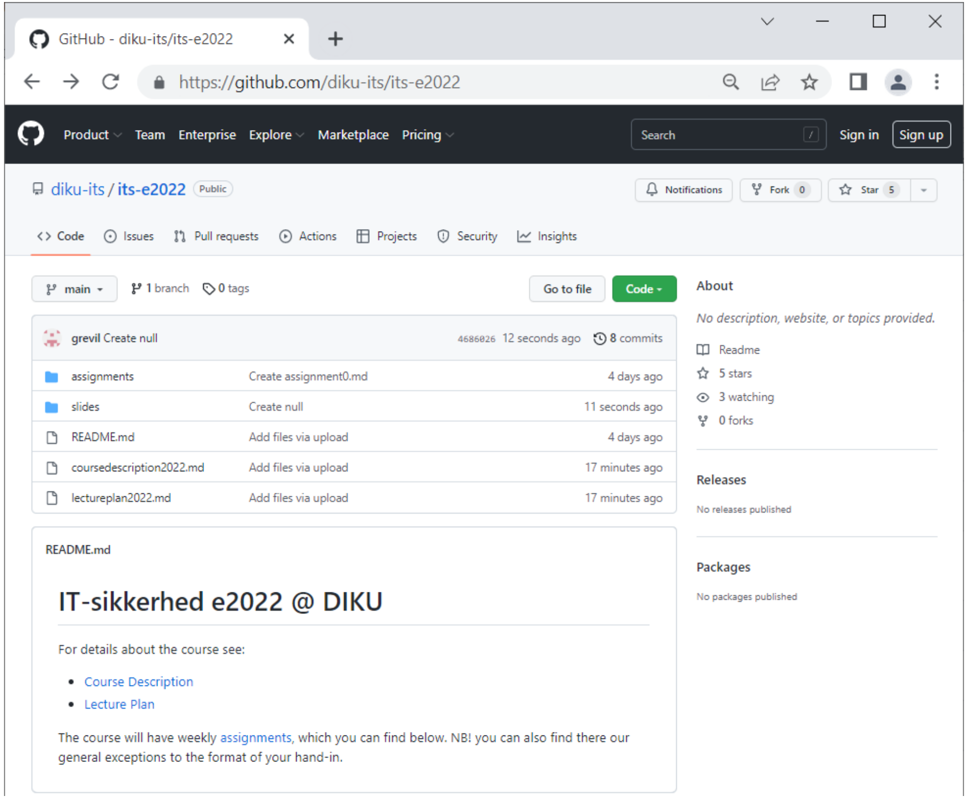
11 Nov 2022

4-hour written exam

All aids allowed except Internet

(Oral re-exam)

Course web site



grevil Create null — 4686026 12 seconds ago — 8 commits

assignments	Create assignment0.md	4 days ago
slides	Create null	11 seconds ago
README.md	Add files via upload	4 days ago
coursedescription2022.md	Add files via upload	17 minutes ago
lectureplan2022.md	Add files via upload	17 minutes ago

About

No description, website, or topics provided.

Readme
5 stars
3 watching
0 forks

Releases

No releases published

Packages

No packages published

README.md

IT-sikkerhed e2022 @ DIKU

For details about the course see:

- Course Description
- Lecture Plan

The course will have weekly assignments, which you can find below. NB! you can also find there our general exceptions to the format of your hand-in.

What you will learn

This course is *not*

- Not a course in how to hack
- Not the latest and greatest in hacks
- Not every aspect of IT-security

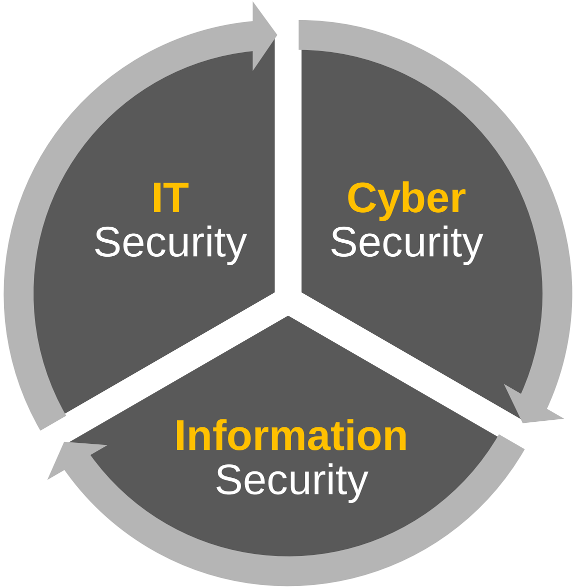
We focus on

- Introduction to the field
- Breadth of topics, some depth
- Getting hands-on (exercises)

Ethics and legal disclaimer

So, what is IT-Security?

Also known as (security, for short)



IT Security

Cyber Security

Information Security

IT-security is many things

Firewalls

Cryptography

Vulnerabilities

Exploits

Malware

Reverse engineering

Passwords

Patching

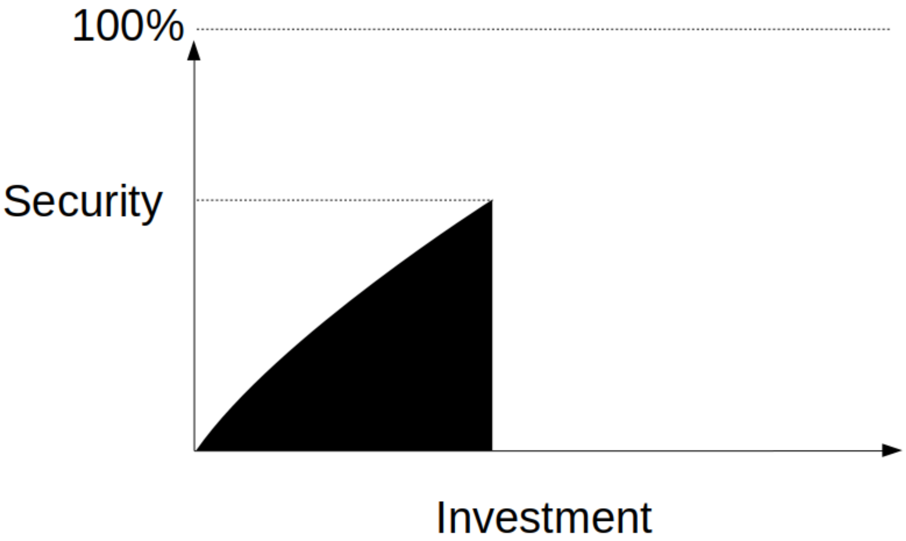
Threat models

Intrusion detection

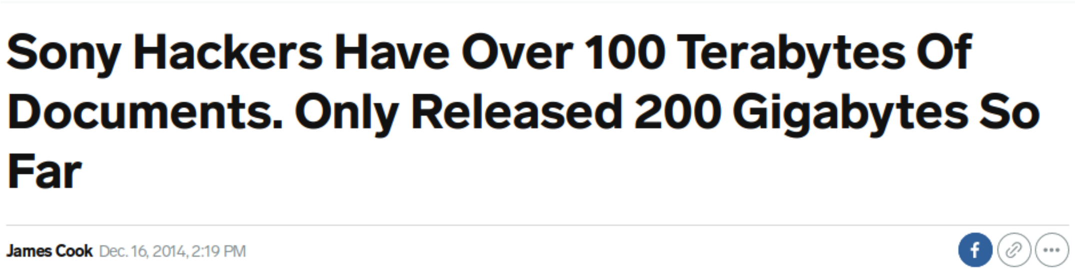
Security management

And much more

100% security is an illusion



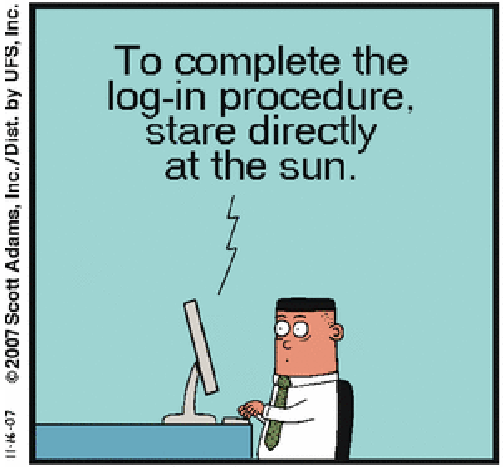
Even big-budget firms get hacked

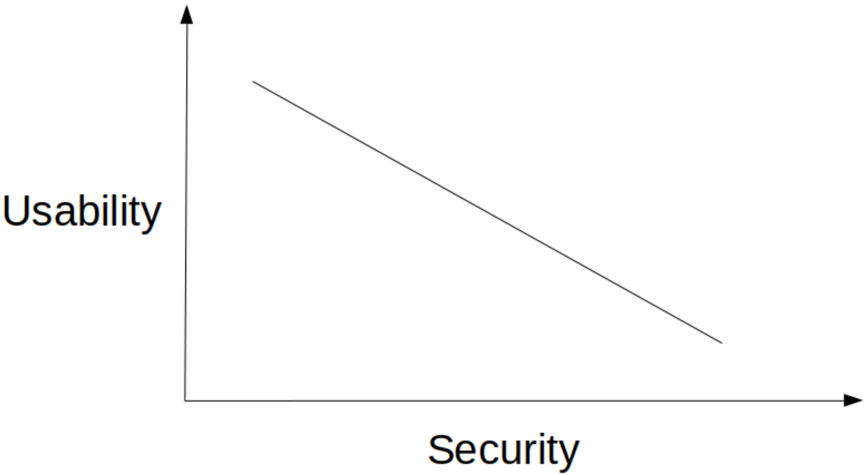


Sony Hackers Have Over 100 Terabytes Of Documents. Only Released 200 Gigabytes So Far

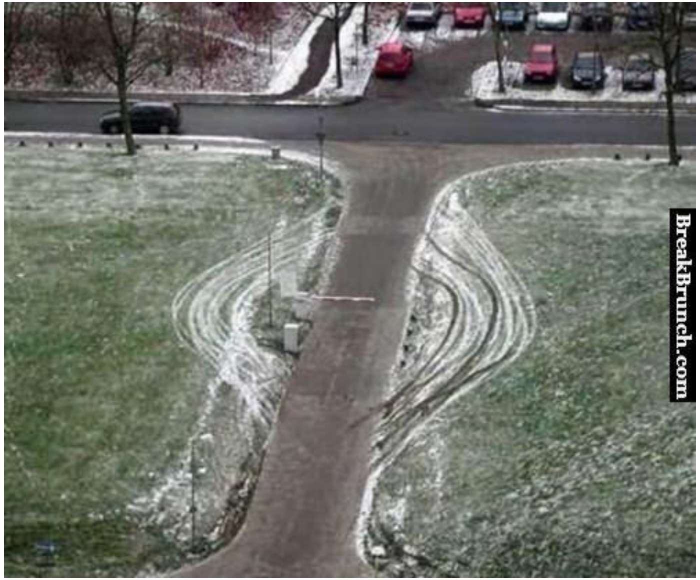
James Cook Dec. 16, 2014, 2:19 PM

Usability – the dual of security?


To complete the log-in procedure, stare directly at the sun.
©2007 Scott Adams, Inc./Dist. by UFS, Inc.
11-16-07



Don’t make security too easy to bypass



Who wins – security or business?

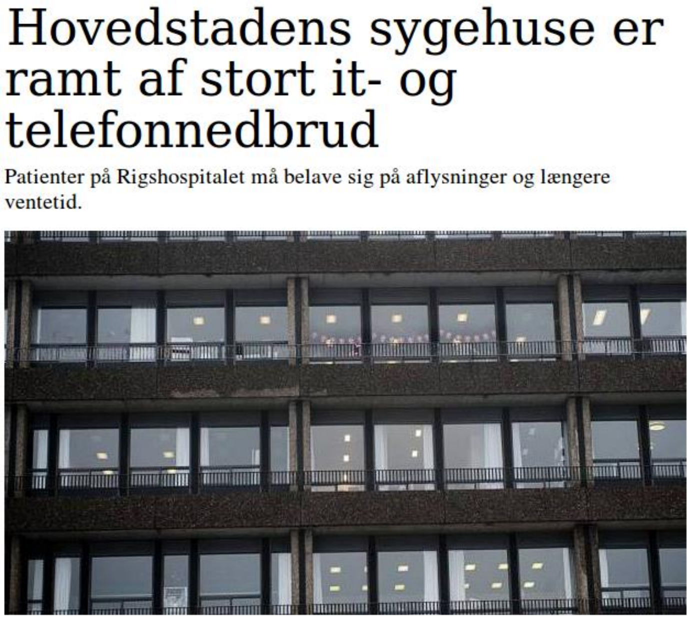
> 69% of users would avoid security controls to make big business deals

BUT security *is* important

Security News This Week: How Shipping Giant Maersk Dealt With a Malware Meltdown

What does IT-security mean to *you*?

Is this security?



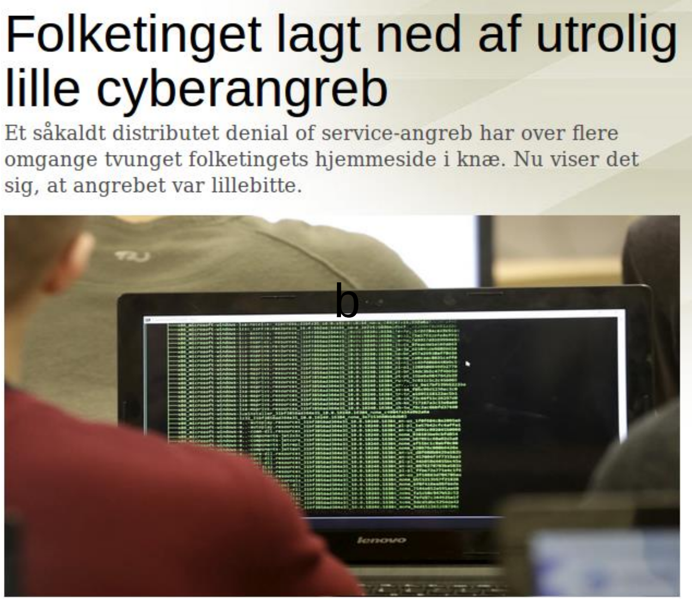
Hovedstadens sygehuse er ramt af stort it- og telefonnedbrud

Patienter på Rigshospitalet må belave sig på aflysninger og længere ventetid.

Is this security?

Massive Flooding Damages
Several NYC Data Centers

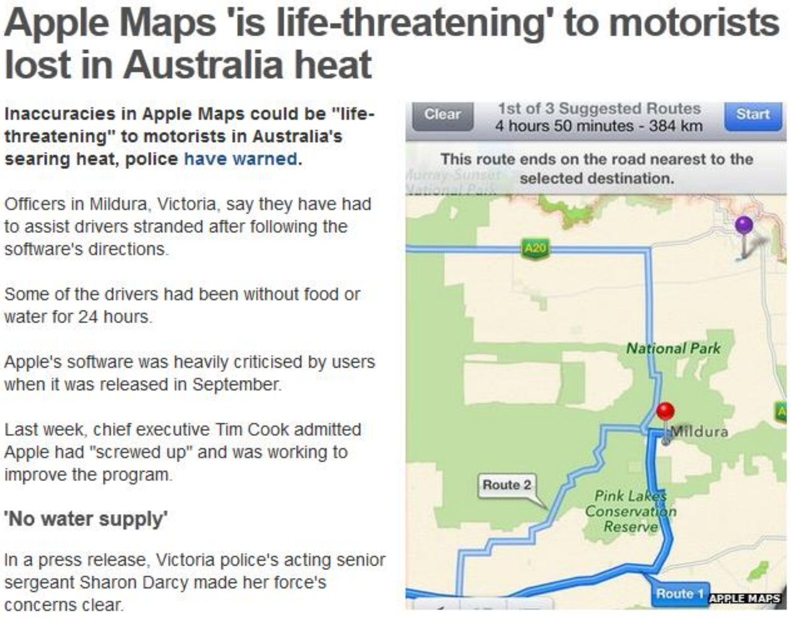
Is this security?



Folketinget lagt ned af utrolig lille cyberangreb

Et såkaldt distributet denial of service-angreb har over flere omgange tvunget folketingets hjemmeside i knæ. Nu viser det sig, at angrebet var lillebitte.

Is this security?



Apple Maps 'is life-threatening' to motorists lost in Australia heat

Inaccuracies in Apple Maps could be "life-threatening" to motorists in Australia's searing heat, police have warned.

Officers in Mildura, Victoria, say they have had to assist drivers stranded after following the software's directions.

Some of the drivers had been without food or water for 24 hours.

Apple's software was heavily criticised by users when it was released in September.

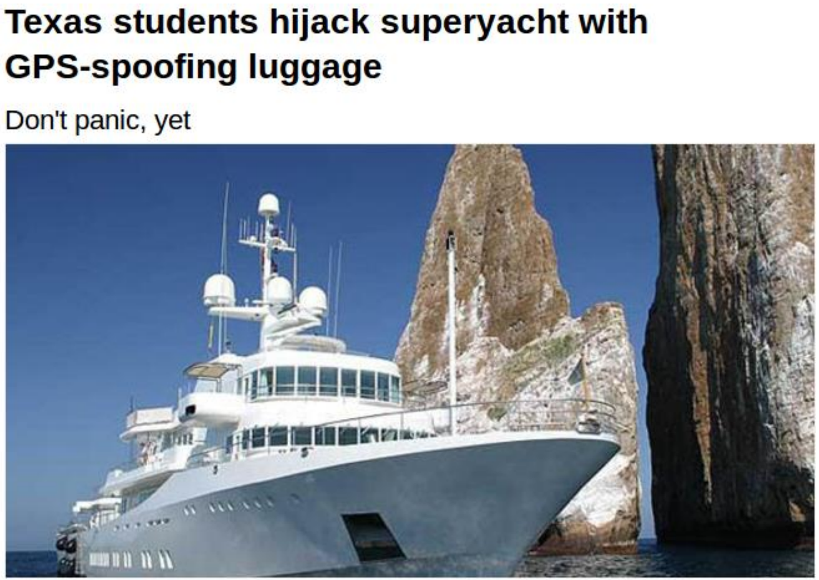
Last week, chief executive Tim Cook admitted Apple had "screwed up" and was working to improve the program.

'No water supply'

In a press release, Victoria police's acting senior sergeant Sharon Darcy made her force's concerns clear.

Clear
1st of 3 Suggested Routes
4 hours 50 minutes - 384 km
Start
This route ends on the road nearest to the selected destination.
Murray-Sunset National Park
A20
National Park
Mildura
Route 2
Pink Lakes Conservation Reserve
Route 1
APPLE MAPS

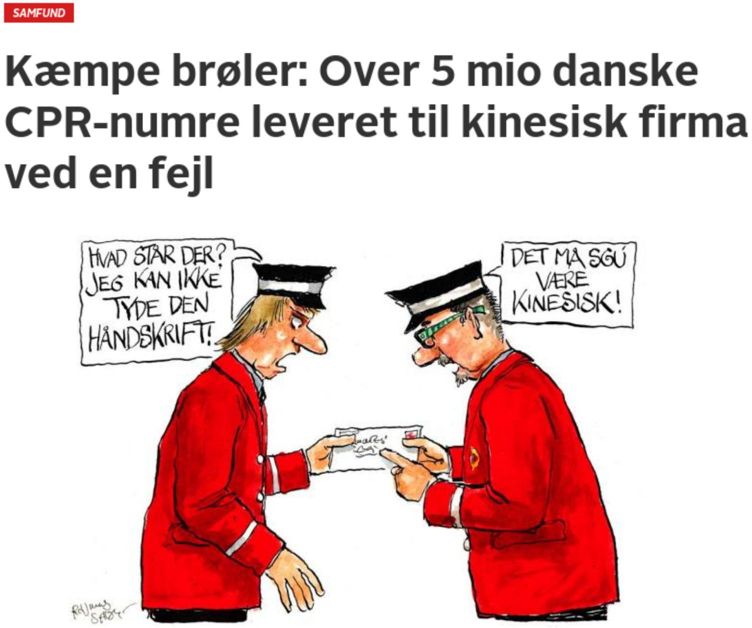
Is this security?



Texas students hijack superyacht with GPS-spoofing luggage

Don't panic, yet

Is this security?

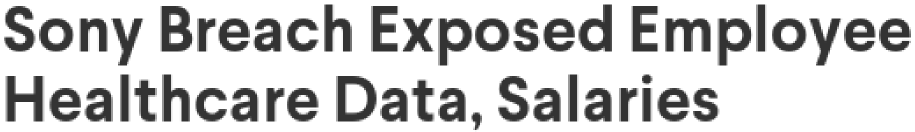


SAMFUND

Kæmpe brøler: Over 5 mio danske CPR-numre leveret til kinesisk firma ved en fejl

HVAD STÅR DER? JEG KAN IKKE TYDE DEN HÅNDSKRIFT!
DET MÅ SGÚ VÆRE KINESISK!

Is this security?



Sony Breach Exposed Employee Healthcare Data, Salaries

Security defined

So, computers fail for many reasons

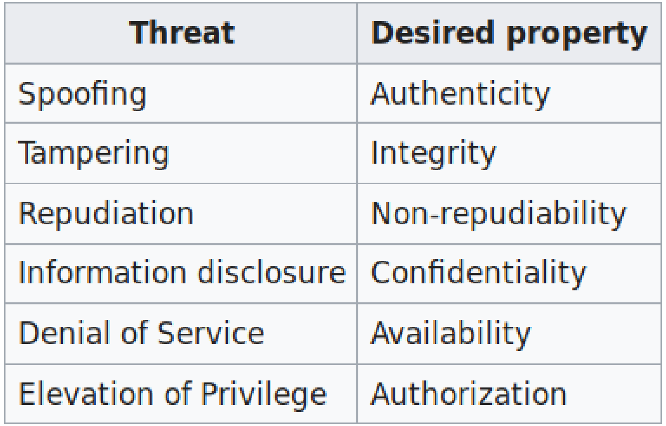
- **Reliability** deals with accidental fails
- **Usability** deals with problems arising from operating mistakes made by users
- **Security** deals with intentional failures made by malicious parties

Security is about computing in the presence of an adversary

A flat tire analogy

Security goals and their threats

The STRIDE threat model helps to answer, "what can go wrong in this system we're working on?"



Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Who hacks?

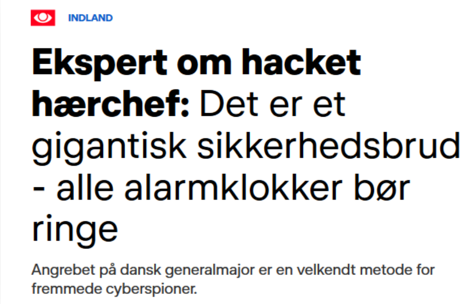
CFCS: the ‘cyber threat’ is very high

FE CENTER FOR CYBERSIKKERHED

Trusselsvurdering:

Cybertruslen mod Danmark 2022

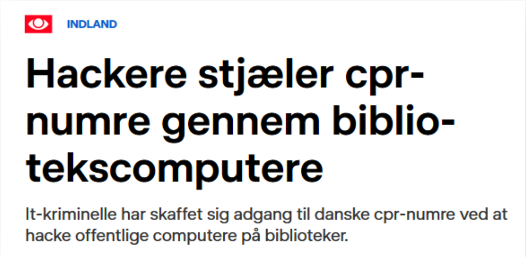
1. udgave juni 2022.



INDLAND

Ekspert om hacket hærchef: Det er et gigantisk sikkerhedsbrud - alle alarmklokker bør ringe

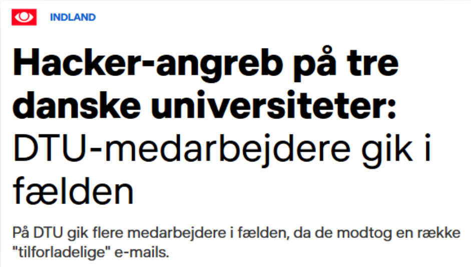
Angrebet på dansk generalmajor er en velkendt metode for fremmede cyberspioner.



INDLAND

Hackere stjæler cpr-numre gennem bibliotekscomputere

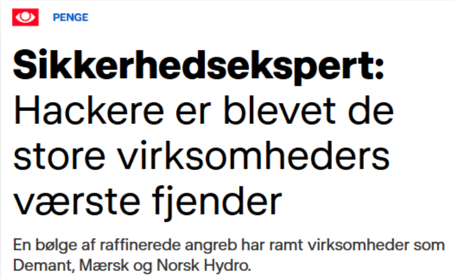
It-kriminelle har skaffet sig adgang til danske cpr-numre ved at hacke offentlige computere på biblioteker.



INDLAND

Hacker-angreb på tre danske universiteter: DTU-medarbejdere gik i fælden

På DTU gik flere medarbejdere i fælden, da de modtog en række "tilforladelige" e-mails.



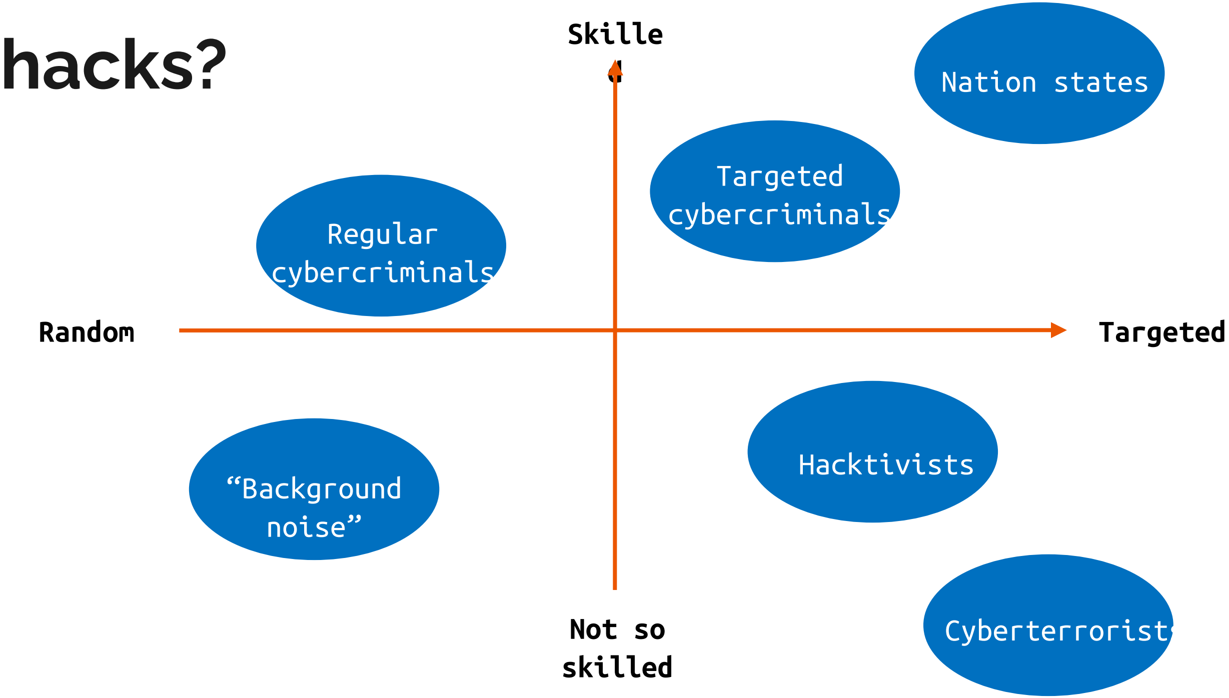
PENGE

Sikkerhedsekspert: Hackere er blevet de store virksomheders værste fjender

En bølge af raffinerede angreb har ramt virksomheder som Demant, Mærsk og Norsk Hydro.

https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-danmark-2022.pdf

Who hacks?



Skille

Nation states

Targeted cybercriminals

Regular cybercriminals

Random

Targeted

“Background noise”

Hacktivists

Not so skilled

Cyberterrorist

Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

Hacktivists

Espionage

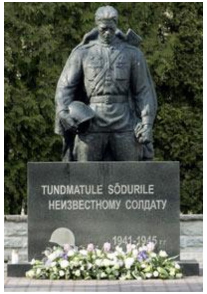
Cyber crime

Cyber war

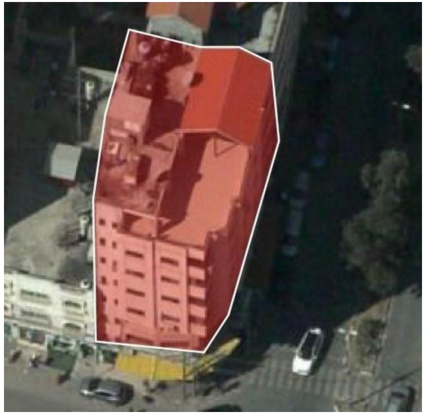
“Actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.”

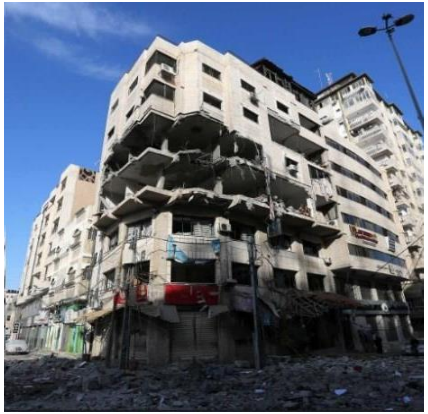
- Richard A. Clarke, tidl. White House Special Advisor

Estonia, 2007

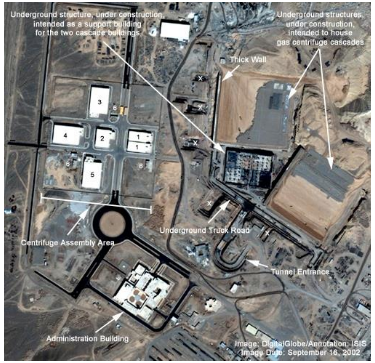


Palestine, 2019





Iran, 2009/10



Underground structure, under construction, intended as a support building for the two cascade buildings
Underground structures, under construction, intended to house gas centrifuge cascades
Thick Wall
3
6
4
2
1
1
6
5
6
X
X
X
X
X
Centrifuge Assembly Area
Underground Truck Road
Tunnel Entrance
Administration Building

Image: DigitalGlobe/Annotation: ISIS
Image Date: September 16, 2002

Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

Hacktivists

Espionage

Cyber crime

Cyber terror

UN: any act "intended to cause death or serious bodily harm to civilians or non-combatants with the purpose of intimidating a population or compelling a government or an international organization to do or abstain from doing any act."

Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

Hacktivists

Espionage

Cyber crime

Hacktivists

Hacktivists false flag operations

Guccifer 2.0 – the attack on Hillary Clinton’s campaign in 2016

Guardians of Peace – the attack on Sony in 2014

Cutting Sword of Justice – the attack on Saudi Aramco in 2012

Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

Hacktivists

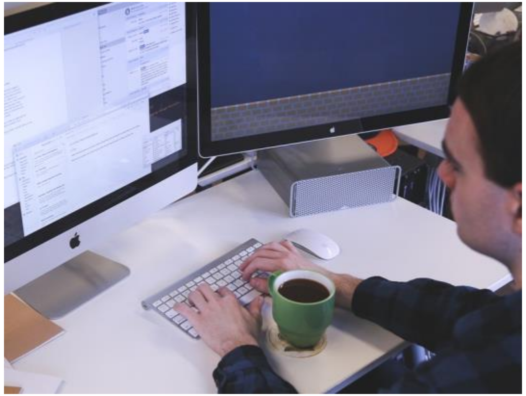
Espionage

Cyber crime

Espionage

Classic

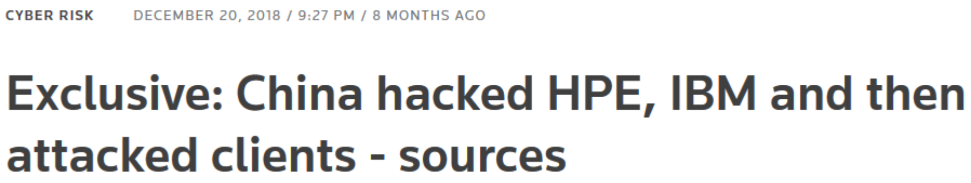
Modern day



Espionage

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
GCHQ
FE
وزارت اطلاعات
جمهوری اسلامی ایران

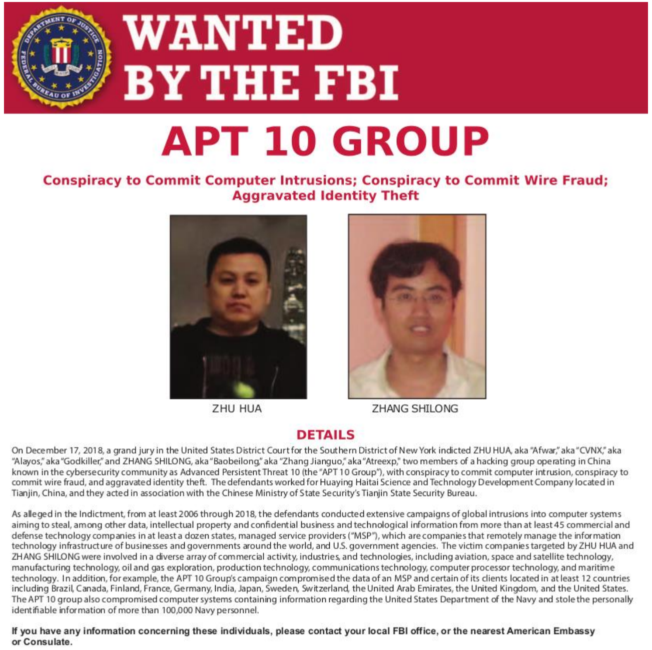
APT10 / STONE PANDA / POTASSIUM / RED APOLLO



CYBER RISK DECEMBER 20, 2018 / 9:27 PM / 8 MONTHS AGO

Exclusive: China hacked HPE, IBM and then attacked clients - sources

FBI’s most wanted - APT10



WANTED BY THE FBI

APT 10 GROUP

Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

ZHU HUA

ZHANG SHILONG

DETAILS

On December 17, 2018, a grand jury in the United States District Court for the Southern District of New York indicted ZHU HUA, aka “Afwar,” aka “CVNX,” aka “Alayos,” aka “Godkiller,” and ZHANG SHILONG, aka “Baobeilong,” aka “Zhang Jianguo,” aka “Atreexp,” two members of a hacking group operating in China known in the cybersecurity community as Advanced Persistent Threat 10 (the “APT 10 Group”), with conspiracy to commit computer intrusion, conspiracy to commit wire fraud, and aggravated identity theft. The defendants worked for Huaying Haitai Science and Technology Development Company located in Tianjin, China, and they acted in association with the Chinese Ministry of State Security’s Tianjin State Security Bureau.

As alleged in the Indictment, from at least 2006 through 2018, the defendants conducted extensive campaigns of global intrusions into computer systems aiming to steal, among other data, intellectual property and confidential business and technological information from more than at least 45 commercial and defense technology companies in at least a dozen states, managed service providers (“MSP”), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, and U.S. government agencies. The victim companies targeted by ZHU HUA and ZHANG SHILONG were involved in a diverse array of commercial activity, industries, and technologies, including aviation, space and satellite technology, manufacturing technology, oil and gas exploration, production technology, communications technology, computer processor technology, and maritime technology. In addition, for example, the APT 10 Group’s campaign compromised the data of an MSP and certain of its clients located in at least 12 countries including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States. The APT 10 group also compromised computer systems containing information regarding the United States Department of the Navy and stole the personally identifiable information of more than 100,000 Navy personnel.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

Hacktivists

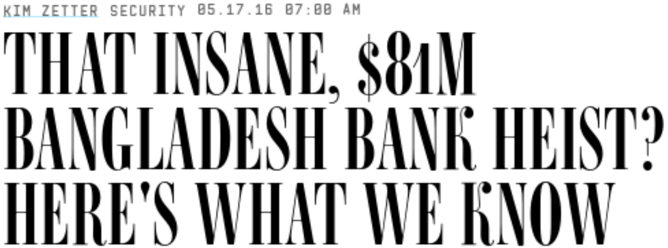
Espionage

Cyber crime

Cyber crime

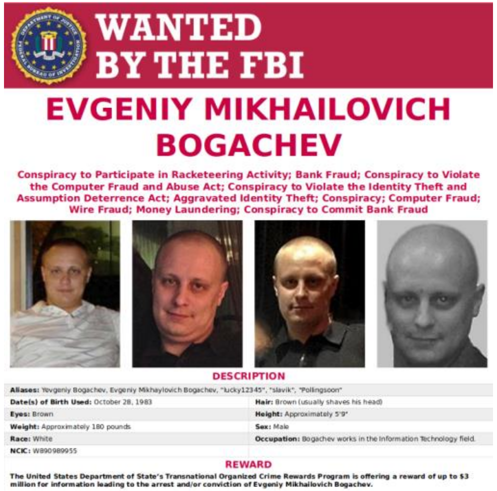
Highly targeted

Less targeted



KIM ZETTER SECURITY 05.17.16 07:00 AM

THAT INSANE, $81M BANGLADESH BANK HEIST? HERE'S WHAT WE KNOW



WANTED BY THE FBI

EVGENIY MIKHAILOVICH BOGACHEV

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

DESCRIPTION

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"	
Date(s) of Birth Used: October 28, 1983	**Hair:** Brown (usually shaves his head)
Eyes: Brown	**Height:** Approximately 5'9"
Weight: Approximately 180 pounds	**Sex:** Male
Race: White	**Occupation:** Bogachev works in the Information Technology field.
NCIC: W890989955	

REWARD

The United States Department of State's Transnational Organized Crime Rewards Program is offering a reward of up to $3 million for information leading to the arrest and/or conviction of Evgeniy Mikhailovich Bogachev.

Who hacks? Or, threats in cyber space

Cyber war

Cyber terror

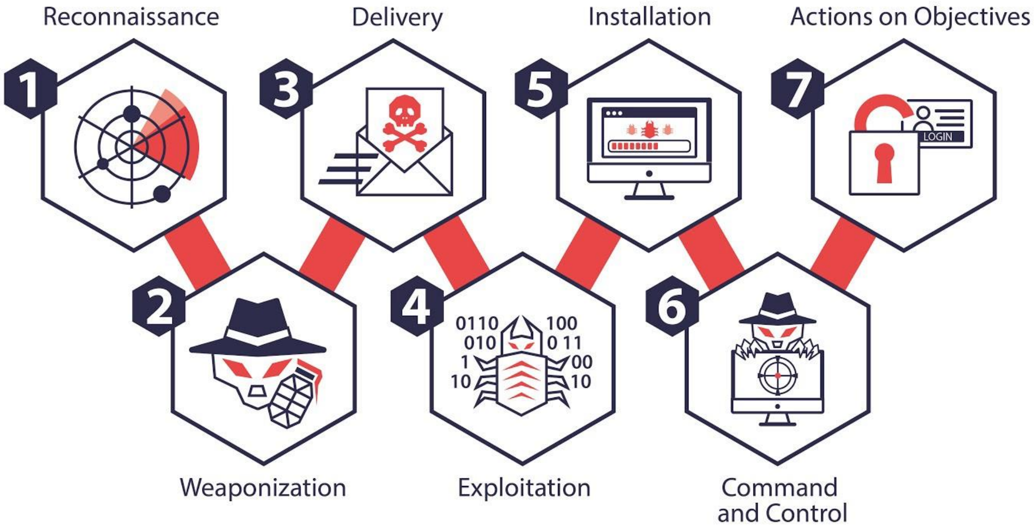
Hacktivists

Espionage

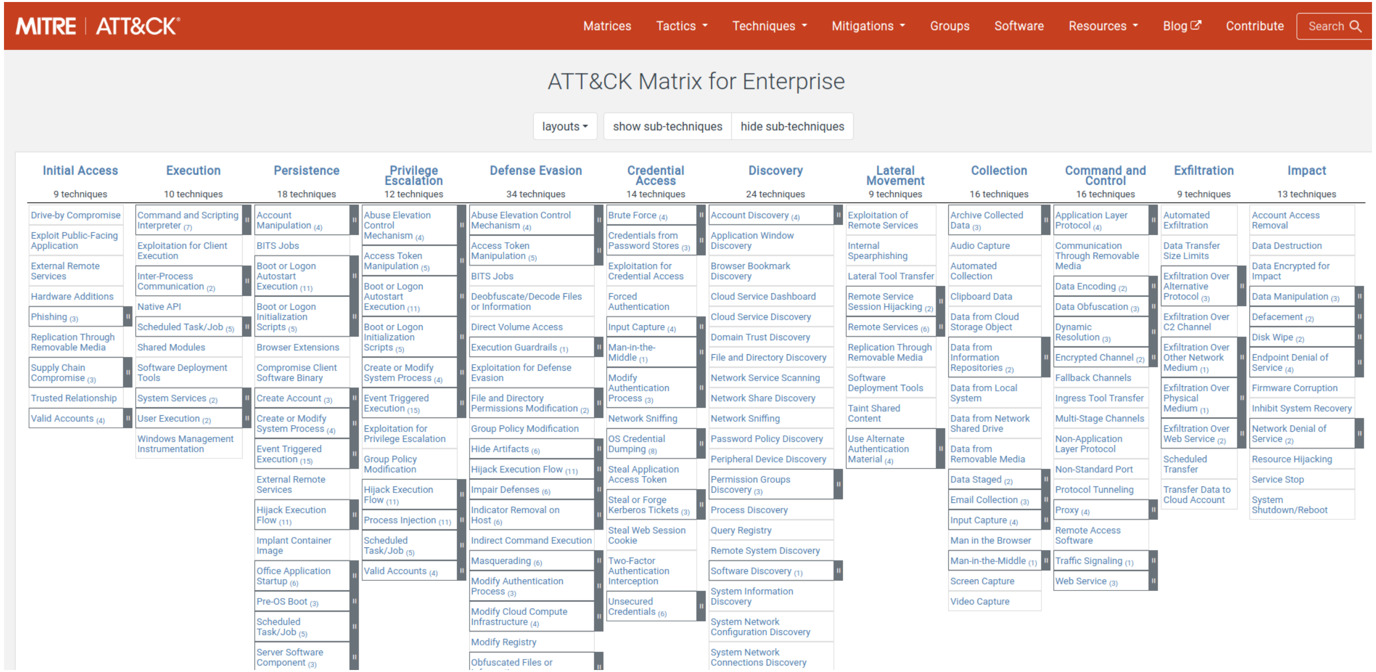
Cyber crime

How hackers hack

The Cyber Kill Chain



Initial Access and MITRE ATT&CK



ATT&CK Matrix for Enterprise

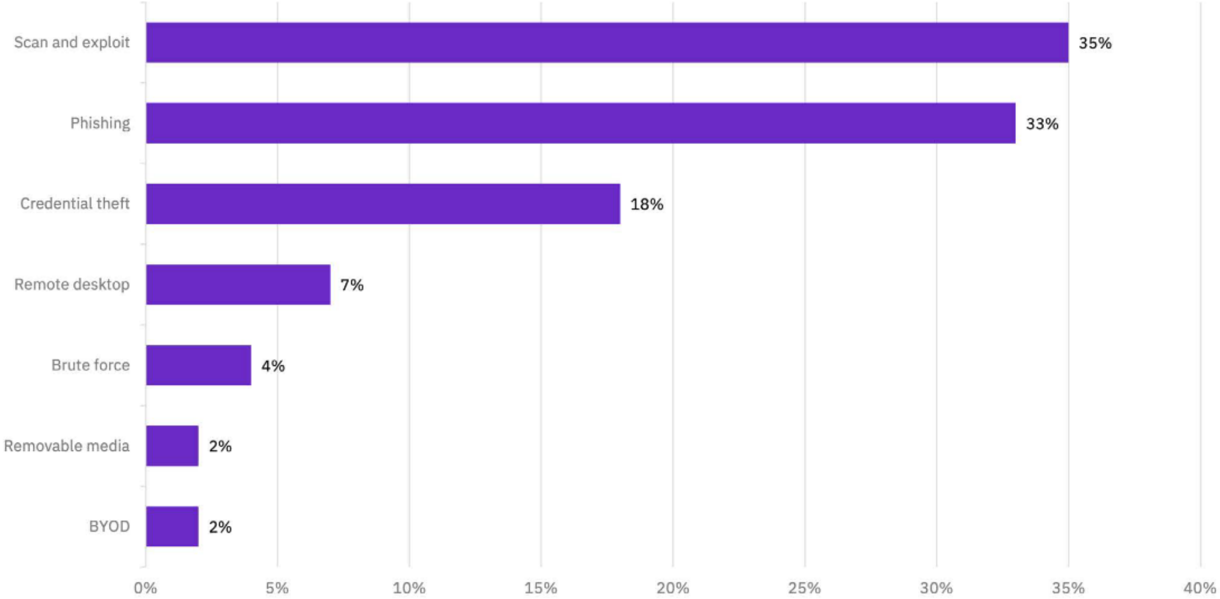
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	24 techniques
Drive-by Compromise	Command and Scripting Interpreter (7)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery
	Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (6)	Steal Application Access Token	Network Sniffing
		Hijack Execution Flow (11)	Scheduled Task/Job (5)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Password Policy Discovery
		Implant Container Image	Valid Accounts (4)	Impair Defenses (6)	Steal Web Session Cookie	Peripheral Device Discovery
		Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Permission Groups Discovery (3)
		Pre-OS Boot (3)		Indirect Command Execution	Unsecured Credentials (6)	Process Discovery
		Scheduled Task/Job (5)		Masquerading (6)		Query Registry
		Server Software Component (3)		Modify Authentication Process (3)		Remote System Discovery
				Modify Cloud Compute Infrastructure (4)		Software Discovery (1)
				Modify Registry		System Information Discovery
				Obfuscated Files or		System Network Configuration Discovery
						System Network Connections Discovery

Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
	Data Staged (2)	Non-Application Layer Protocol		Network Denial of Service (2)
	Email Collection (3)	Non-Standard Port		Resource Hijacking
	Input Capture (4)	Protocol Tunneling		Service Stop
	Man in the Browser	Proxy (4)		System Shutdown/Reboot
	Man-in-the-Middle (1)	Remote Access Software		
	Screen Capture	Traffic Signaling (1)		
	Video Capture	Web Service (3)		

Look at the numbers (initial access)

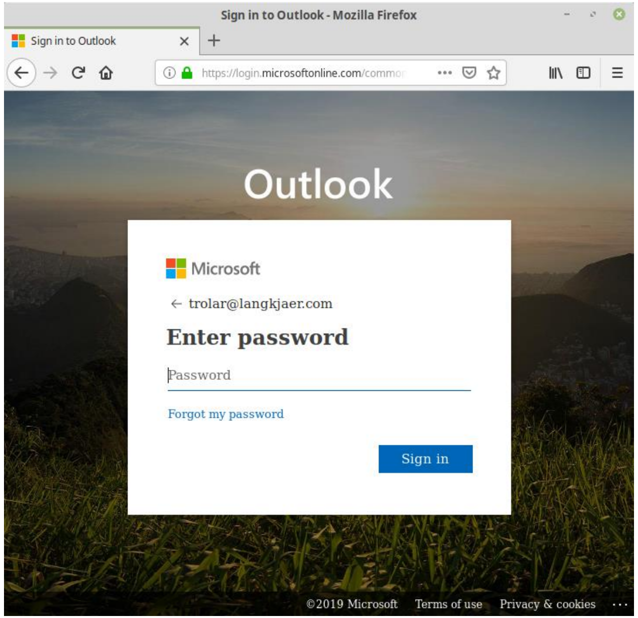
X-Force Threat Intelligence Index 2021

IBM



https://www.ibm.com/security/data-breach/threat-intelligence

#3: Credential theft


Sign in to Outlook - Mozilla Firefox

Sign in to Outlook

https://login.microsoftonline.com/commo

Outlook

Microsoft

← trolar@langkjaer.com

Enter password

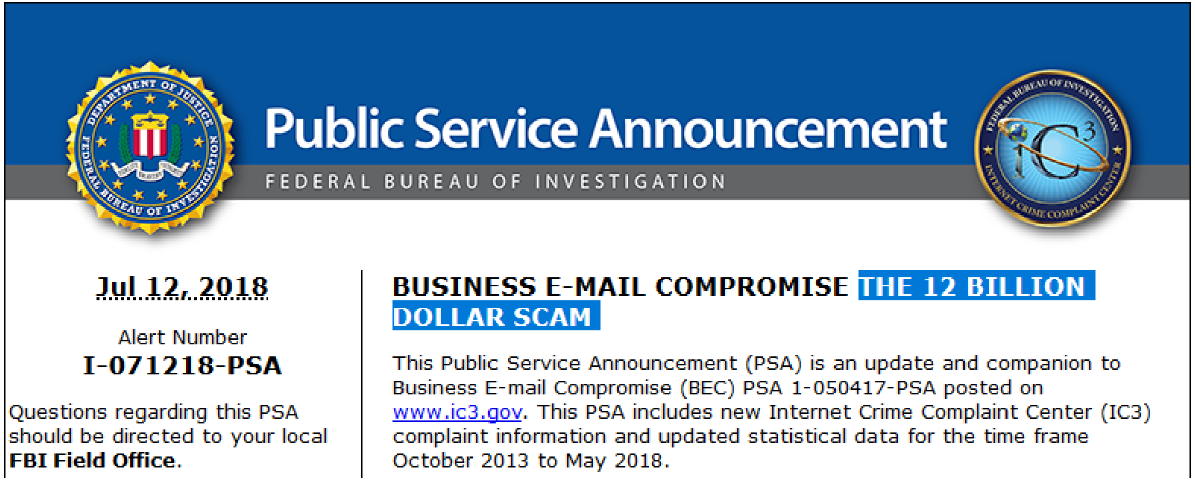
Password

Forgot my password

Sign in

©2019 Microsoft Terms of use Privacy & cookies ...

BEC is where the money’s at



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Jul 12, 2018

Alert Number

I-071218-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update and companion to Business E-mail Compromise (BEC) PSA 1-050417-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data for the time frame October 2013 to May 2018.

Case story

CEO of Danish company with 100 employees

Two fake emails, $600K and $40K, sent to accounting

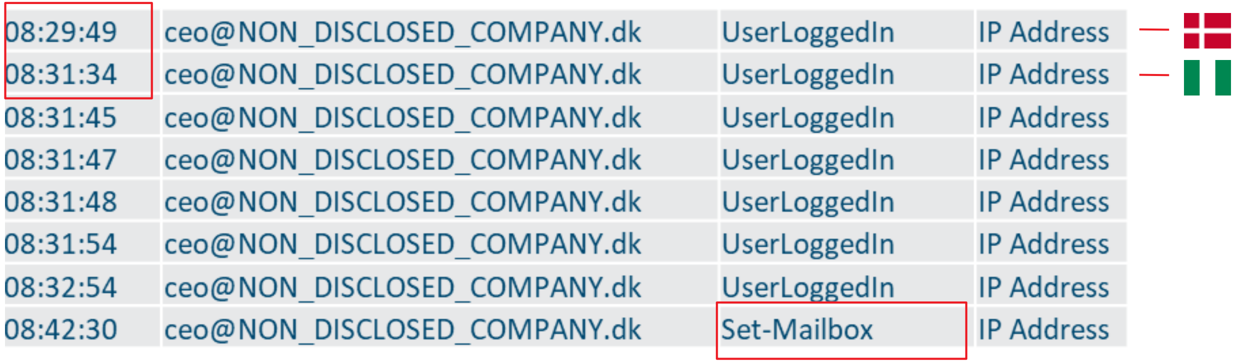
Attackers logged in from Nigeria while CEO logged in from Denmark

Unclear how password was stolen

Created automatic rules to delete replies from accounting

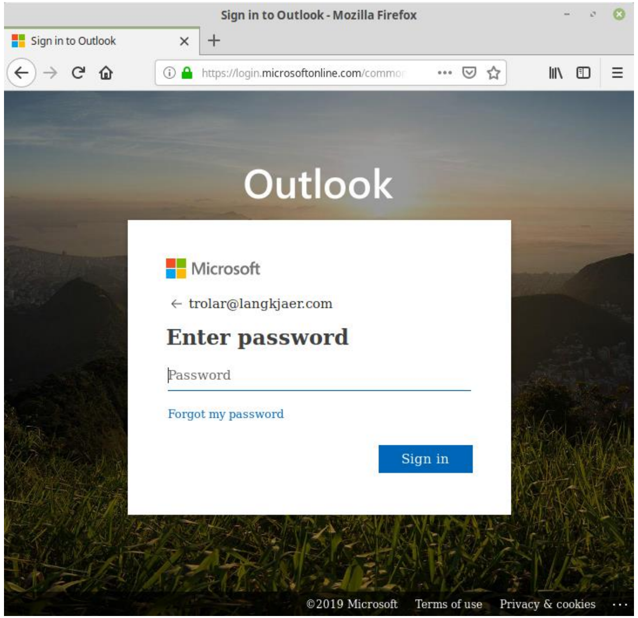
Almost perfect Danish

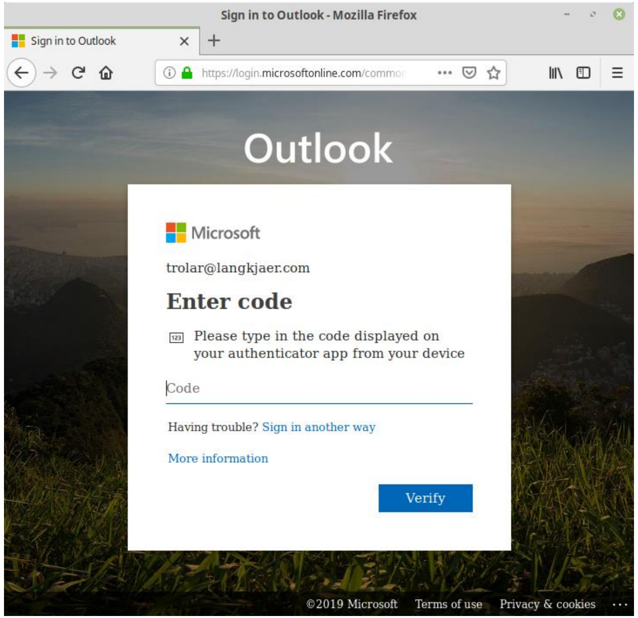
Case story: “While CEO logged in from Denmark”



08:29:49	ceo@NON_DISCLOSED_COMPANY.dk	UserLoggedIn	IP Address	🇩🇰
08:31:34	ceo@NON_DISCLOSED_COMPANY.dk	UserLoggedIn	IP Address	🇳🇬
08:31:45	ceo@NON_DISCLOSED_COMPANY.dk	UserLoggedIn	IP Address	
08:31:47	ceo@NON_DISCLOSED_COMPANY.dk	UserLoggedIn	IP Address	
08:31:48	ceo@NON_DISCLOSED_COMPANY.dk	UserLoggedIn	IP Address	
08:31:54	ceo@NON_DISCLOSED_COMPANY.dk	UserLoggedIn	IP Address	
08:32:54	ceo@NON_DISCLOSED_COMPANY.dk	UserLoggedIn	IP Address	
08:42:30	ceo@NON_DISCLOSED_COMPANY.dk	Set-Mailbox	IP Address	

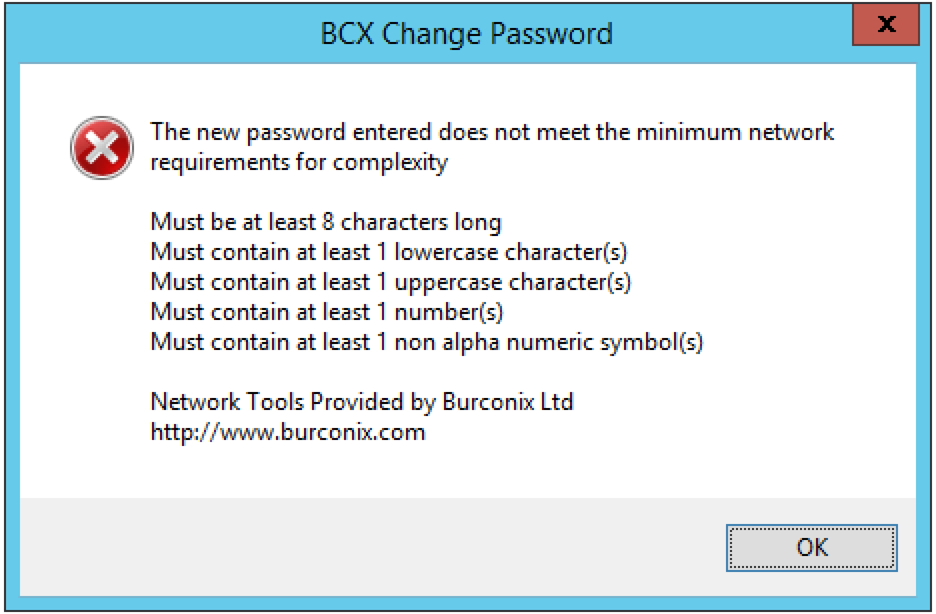
Solution




Sign in to Outlook - Mozilla Firefox
Sign in to Outlook
https://login.microsoftonline.com/commo
Outlook
Microsoft
trolar@langkjaer.com
Enter code

Please type in the code displayed on your authenticator app from your device

Not the solution

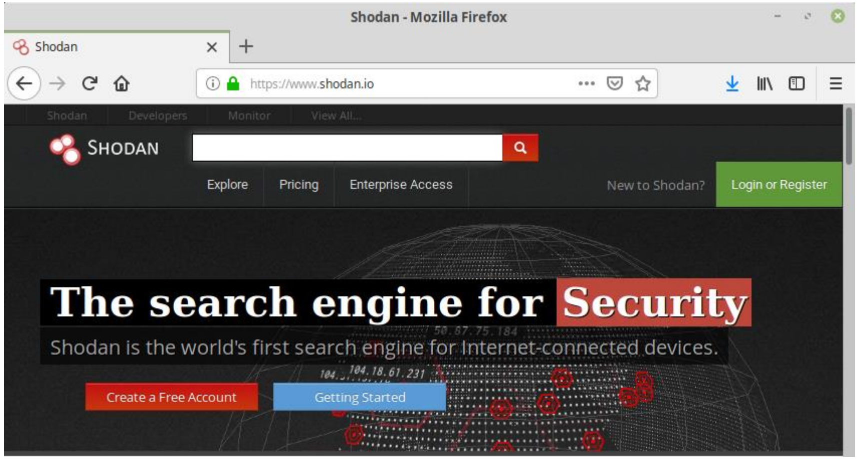


The new password entered does not meet the minimum network requirements for complexity

Must be at least 8 characters long
Must contain at least 1 lowercase character(s)
Must contain at least 1 uppercase character(s)
Must contain at least 1 number(s)
Must contain at least 1 non alpha numeric symbol(s)

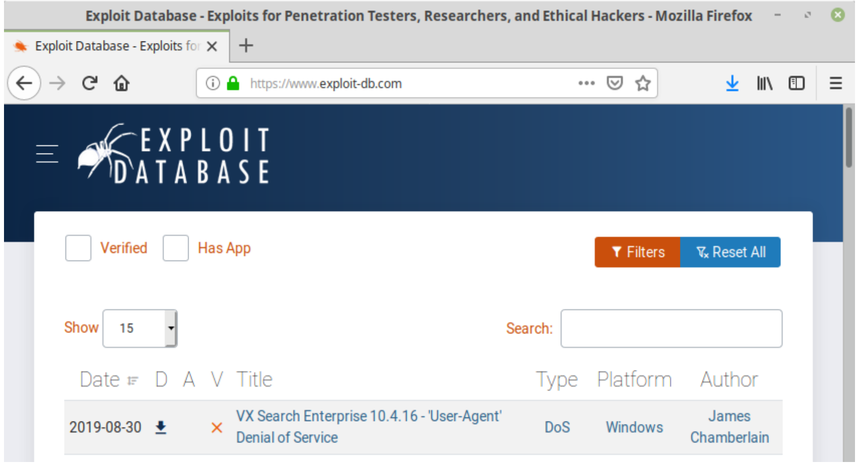
Network Tools Provided by Burconix Ltd
http://www.burconix.com

#2: Scan and exploit



The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.


Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers - Mozilla Firefox
Exploit Database - Exploits for
https://www.exploit-db.com
EXPLOIT DATABASE
□ Verified
□ Has App
Filters
Reset All
Show 15
Search:

Date	D	A	V	Title	Type	Platform	Author
2019-08-30	⬇		✕	VX Search Enterprise 10.4.16 - 'User-Agent' Denial of Service	DoS	Windows	James Chamberlain

Do It Yourself (DIY)

Find a new vulnerability and exploit it

(Later)

What to do?

Study the body of knowledge

Study how breaches occur

Implement the right security controls for your situation

That matches the likelihood and consequences of the threats that you face

And most importantly:

Keep coming to class! ;)